EUROPEAN COMMISSION
European Education and Culture Executive Agency

RECORD OF PERSONAL DATA PROCESSING

Art. 31 REGULATION (EU) 2018/1725 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (henceforth the "Regulation")

Record nº *01-2023*

In accordance with Article 31 of Regulation 2018/1725, individuals whose personal data are processed by the Agency in any context whatsoever are to be protected with regard to the processing of personal data and the Agency has to keep records of their processing operations.

This record covers two aspects:
1. Mandatory records under Art 31 of the Regulation (recommendation: make the header and part 1 publicly available)
2. Compliance check and risk screening (initial; part 2 is internal only to the Agency, not published)

The ground for the record is (tick the relevant one):

☐ *Regularization of a data processing operation already carried out*
☒ *Record of a new data processing operation prior to its implementation*
☐ *Change of a data processing operation*
☐ *Migration from notification to record.*

Processing of personal data under the European Voluntary Humanitarian Aid Corps Training	
1	**Last update of this record (where applicable)**
	N/A
2	**Short description of the processing**
	The processing of personal data happens in the frame of the European Voluntary Humanitarian Aid Corps Training, implemented by EACEA's contractor Lattanzio Kibs. The processing is required to allow European Solidarity Corps (ESC) registered users in the European Youth Portal to gain access to EU Academy and complete: - The self-assessment questionnaire to reflect on their motivation to the action; - The online training courses which consists of 17 modules; - The online test to evaluate the learning; - The face-to-face training scheduler for those who have succeeded the online test.

	Data will also be processed when analysing responses to a course survey on the EU Academy platform, analysing online test responses and collecting statistics and reports in anonymised format on the use of the courses. Finally, personal data is processed when the candidates having succeeded the online test fill in their details in the training scheduler. This data is extracted by the contractor from EU Academy, as it is needed for logistical arrangements of the face-to-face training.
Part 1 - Article 31 Record	
3	**Name of the Controller** **Unit(s) and/or function of person acting on behalf of the Controller**
	Controller: European Education, and Culture Executive Agency Unit A5: Youth, EU Solidarity Corps and Aid Volunteers Head of Unit: EACEA-SOLIDARITY-CORPS@ec.europa.eu
4	**Contact details of the Data Protection Officer (DPO)**
	EACEA-data-protection@ec.europa.eu.
5	**Name and contact details of joint controller (where applicable)**
	Not applicable
6	**Name and contact details of processor (where applicable)**
	LATTANZIO KIBS S.p.A (consortium leader) Statutory registration number: MI-2506743 Via D. Cimarosa 4, 20144 Milan, Italy DPO: Dr. Francesco Martinotti dpo@lattanziokibs.com INSTITUT BIOFORCE (partner) Statutory registration number: SIRET n° 340 402 00033 41 Avenue du 8 mai 1945, 69200 Venissieux, France DPO : Marianne Le Floch mlefloch@bioforce.org Instituto de Estudios sobre Conflictos y Accion Humanitaria – IECAH (Partner) Statutory registration number: 167779 Calle Jaén 13, 28020 Madrid, Spain DPO : Paula Foix – paula.foix@iecah.org RUHR-UNIVERSITAET BOCHUM (Partner) Statutory registration number: n/a Universitaetsstrasse 150, 44801 Bochum, Germany DPO : Mr. Robin Pass – robin.pass@rub.de FONDAZIONE PUNTO.SUD (Partner) Statutory registration number: MI-2001697 Via Angera 3, 20125 Milan, Italy Data Processor: Fabrizio Alberizzi puntosud@puntosud.org ACI BLUETEAM S.p.A. (sub-contractor) Statutory registration number: RM-1603827 Via Marsala 8, 00185 Rome, Italy Paolo Bertola privacy@aciblueteam.it

7	**Purpose of the processing**
	Data processing is necessary for the following purposes: A. To ensure access for European Solidarity Corps registered users to the following contents on EU Academy and allow them to implement the related activities: the self-assessment questionnaire, the set of courses of the European Voluntary Humanitarian Aid Corps Training, the online test and the face-to-face training scheduler for those who passed the test. B. To enable reporting for the European Solidarity Corps services of DG EAC and EACEA, as well as to be able to present an aggregated analysis of course usage and of survey responses, by key characteristics of users, in statistical reports. The data is anonymised for this last purpose. C. To present an analysis of the online test's responses and of the face-to-face training scheduler to EACEA, EAC and the contractor, including by key characteristics of respondents. D. To enable the contractor to plan the face-to-face training, to book travel for successful candidates to travel to and from the training centre and to process travel reimbursements. E. To provide information to the training providers about special needs related to health conditions or learning difficulties of participants, in order to ensure appropriate support during the face-to-face training.
8	**Description of the categories of data subjects**
	Whose personal data are being processed? ☐ Agency staff (Contractual and temporary staff in active position) ☐ Visitors to the Agency ☐ Contractors providing goods or services ☐ Applicants ☐ Relatives of the data subject ☐ Complainants, correspondents and enquirers ☐ Witnesses ☐ Beneficiaries ☐ External experts ☐ Contractors ☒ Other, please specify: Registered users on the European Youth Portal interested in the European Voluntary Humanitarian Aid Corps, including successful candidates having passed the online test and enrolled in the face-to-face training.
9	**Description of personal data categories**
	a) Categories of personal data: ☐ in the form of personal identification numbers ☐ concerning the physical characteristics of persons as well as the image, voice or fingerprints ☐ concerning the data subject's private sphere ☒ concerning pay, allowances and bank accounts

☐ concerning recruitment and contracts

☒ concerning the data subject's family

☐concerning the data subject's career

☐ concerning leave and absences

☒ concerning missions and journeys

☐ concerning social security and pensions

☐ concerning expenses and medical benefits

☒ concerning telephone numbers and communications

☒ concerning names and addresses (including email addresses)

☒ Other: please specify: _____

1. European Solidarity Corps registered users' data indicated below are transferred from the European Youth Portal to EU Academy:
   - Email
   - EU Login username
   - First name
   - Last name
   - Contact language
   - Country of residence
   - City

2. The following data available on EU Academy may be processed:
   - Replies to self-assessment questionnaire
   - course enrolment data,
   - course access and course completion data,
   - course progress data
   - replies to course survey
   - online test responses
   - data filled in training scheduler.

3. The following data, extracted from the scheduling solution on EU Academy, filled in by candidate volunteers for the purposes of logistical arrangements and follow-up related to the face-to-face training will be processed:

   First name
   Last name
   Email address
   Mobile number
   Sex
   Date and place of birth
   Place of departure
   Special dietary needs
   Special access requirements
   Special assistance needs due to personal health conditions or learning difficulties
   One emergency contact: name, relationship, telephone number

4. The following data will be processed by the travel agency organising the travel to the face-to-face training:

   Name and surname
   Date and place of birth
   Nationality
   Sex

	Place of departure Information on health, dietary needs and special assistance, if relevant 5. Data collected via an expenses form for travel costs (to be filled only by those candidate volunteers who make an expense claim) will be processed: - Name - Address - Telephone Number - Email - Name of Bank - Name of Bank Account - IBAN Number - SWIFT/BIC Number ***b) Categories of personal data processing likely to present <u>specific risks:</u>*** ☐ data relating to suspected offences, offences, criminal convictions or security measures ☒ data being used to evaluate personal aspects of the data subject (ability, efficiency, conduct) In the self-assessment, candidates will evaluate themselves regarding their capacity to volunteer in the field of humanitarian aid. ***c) Categories of personal data whose processing is <u>prohibited</u>, with exceptions (art. 10):*** ☐ revealing racial or ethnic origin ☐ revealing political opinions ☐ revealing religious or philosophical beliefs ☐ revealing trade-union membership ☒ concerning health ☐ genetic data, biometric data for the purpose of uniquely identifying a natural person ☐ concerning sex life or sexual orientation The training scheduler will require information on: Special dietary needs Special access requirements Special assistance needs due to personal health conditions or learning difficulties ***d) Specify any additional data or explanatory information on the data being processed, if any:***
10	**Retention time (time limit for keeping the personal data)**
	For the purposes set out in 7 A, the period of storage, including access logs, is defined by the retention period of the European Youth Portal. Personal data contained within user accounts of the European Solidarity Corps will be deleted three years after they reach the upper age limit of eligibility for participation in the Corps, unless the user has agreed to join any alumni scheme that may be in place at that time, has expressed via email an interest / consent in keeping the user account or has benefited from EU funding through participating in the programme in which case the data is kept for 5 years from the last financial transaction according to the common retention list.

	The retention policy of EU Academy applies to the retention of personal data in the EU Academy environment for the purposes defined in 3 A, B and C. The personal data processed for purposes 7 D and E will be deleted from the data processors' and sub-processors' servers within the 6 months following the completion of the last specific contract under Framework Contract SI2.3217. **Is any further processing for historical, statistical or scientific purposes envisaged?** ☐ yes ☒ no **If yes, indicate the further retention time:** N/A
11	**Recipients of the data**
	Access to personal data may be given on a need-to know basis to the following recipients: • Designated staff of the European Commission, in particular Directorate General Education and Culture (DG EAC) and JRC (EU Academy team); • Designated staff of EACEA; • Authorised staff of the contractor of the Framework services contract n° SI2.3217 consortium led by Lattanzio Kibs and composed of Institut Bioforce, Fondazione Punto.Sud, Ruhr-Universität Bochum, Instituto de Estudios sobre Conflictos y Accion Humanitarian. • ACI BLUETEAM S.p.A. (sub-contractor) The transfer of data to other third parties is prohibited. Personal data collected will never be used for marketing purposes. In addition, in case of control or dispute, personal data can be shared with and processed by the bodies charged with a monitoring or inspection task in application of Union law in compliance with the applicable data protection rules and within the scope of their tasks entrusted by the relevant legislation. This includes, in particular, the following recipients: - The European Court of Justice or a national judge as well as the lawyers and the agents of the parties in case of a legal procedure; - The European Anti-Fraud Office (OLAF); - The Internal Audit Service of the Commission - The Investigation and Disciplinary Office of the Commission (IDOC) - The European Court of Auditors - The European Ombudsman - The European Public Prosecutor's Office - EU courts and national authorities
12	**Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?**
	No data transfers to third countries
13	**General description of the technical and organisational security measures**
	The European Youth Portal is under the responsibility of DG EAC (for purpose A), and the applicable measures are described in the dedicated data protection record. EU Academy is under the responsibility of JRC (for purposes B and C) and the applicable measures are described in the dedicated data protection record. For purposes D and E, the following security measures are applied:

The Consortium led by Lattanzio KIBS proceeded, with a working group composed of their DPOs and experts in the organization and security systems, in monitoring compliance with European legislation through constant observation of the results achieved and subsequent continuous review, in order to ensure always over time the risk mitigation and compliance of the treatment with the General Data Protection Regulation 2016/679 and Regulation 2018/1725 (EUDPR), even in the face of changes to which all treatments are subject (internal and external context, purpose of processing, tools used, business organization, etc.).

Each consortium member has its own internal organization to meet the requirements of European data processing law.

LATTANZIO KIBS:

The company has taken measures to ensure safety in the following areas:

• Authorised appointments
All employees and consultants of Lattanzio KIBS at the time of signature the contract of employment or professional assignment, are appointed as "authorized to process personal data". This act of appointment is mandatory through the signing of a special form containing the information to the employee pursuant to Article 13 of the European Regulation 2016/679.

• Standards for the use of business information systems
To regulate the correct use of company information systems, a "Regulation for the use of information systems and data protection" has been drawn up. The Regulation, of which adequate information and training is given, applies to employees and all those who have access to information systems.
All employees, consultants and collaborators must view, know and adapt their behaviour to the Internal Privacy Regulations.

• Protection of the computer system
The highest standards are expected in terms of continuity and energy supply, environmental conditioning, fire protection system and physical and logical safety management. Access to the Server Farm goes through a solid system of access control to the structure to prevent any intrusion by unauthorized persons.

On all corporate servers and in particular on the Terminal Servers to which users connect in Remote Desktop mode to access the corporate file system is installed an antivirus/ antimalware program, with automatic updates enabled, to detect and block the presence of any local threats. To protect the infrastructure from network attacks, there is a new generation firewall.

PUNTOSUD:

The company has taken measures to ensure safety in the following areas:

• Authorised appointments
Selected employees are appointed as "authorized to process personal data" through the signing of a special form containing the information to the employee pursuant to Article 13 of the European Regulation 2016/679.

• Standards for the use of business information systems
To regulate the correct use of company information systems, a "Regulation for the use of information systems and data protection" is in place and shall be accepted by all the employees at the time of their hiring.

• Protection of the computer system
PuntoSud IT system has been recently refreshed to guarantee the highest standards of security and protection. Access to the new server is protected by a Sophos XGs firewall. A VPN SSL is in place to guarantee remote access to all the employees.
Antivirus/ antimalware program, with automatic updates enabled, are installed on all devices.

IFHV / RUHR-UNIVERSITY BOCHUM

The successful execution of the Ruhr-Universität Bochum's business processes in research, teaching and administration is highly dependent on reliably functioning information and communication technology (IT). This results in high demands on the availability, confidentiality and integrity of the processed information, IT procedures and IT systems of the Ruhr-Universität Bochum.

In order to meet this demand, the Rectorate of the Ruhr-Universität Bochum has appointed a Coordination Committee for Information Security. The Coordination Committee has developed a guideline for information security. This describes guiding principles, strategies and measures (rules) for securing information processing. The defined measures take into account the special situation of cooperative and respectful interaction in a university environment.

In the guideline for information security at the Ruhr-Universität Bochum, the rectorate has defined the principles for structuring information security at the Ruhr-Universität Bochum. Based on these principles, the following chapters of this framework concept describe strategies and measures that serve to secure information processing at the Ruhr-Universität Bochum. They are based on the requirements of the internationally recognized standards DIN ISO/IEC 27001/27002.2

Organizational structure of information security

At the Ruhr-Universität Bochum, a multi-level organizational structure for information security has been established, consisting of a staff unit of the rectorate (headed by the central information security officer), the coordination committee and the decentralized information security officers. All institutions are recommended to appoint a decentralized information security officer. Otherwise, the management of the institution performs this function. The appointment must be made in writing and by mutual agreement and must be withdrawn if the assignment is changed.

The decentralized information security officers must be involved at an early stage in the planning phase for the introduction or modification of IT-supported business processes at their institution. The central information security officer shall be involved on request in the introduction or modification of IT-supported business processes with cross-institutional effects and in other procedures.

Responsibility

The management of the Ruhr-Universität Bochum bears the overall responsibility for information security at the Ruhr-Universität Bochum. It must ensure that the institutions of the Ruhr-Universität Bochum are able to implement appropriate information security at their institution. Within this framework, the management of each institution bears responsibility for information security at its institution.

The management of each institution shall ensure that the need for protection with regard to confidentiality, integrity and availability of the IT applications and IT components used and the information processed thereby is correctly determined and that appropriate security measures are implemented. The tasks for implementing the security measures must be clearly assigned.

BIOFORCE:

The Bioforce IT system is secured and the data is stored on a Microsoft cloud, with servers based in the EU (France). Only authorized staff can have access to the data. The cloud is secured. Antivirus, spam and web filters are used on IT materials and a network monitor is used. IT material are locked. Archives are stored in a secured locked room only accessible by authorized staff.

IECAH:
IECAH is the sole one responsible for data treatment.
The purpose of data treatment is only the project to which it was submitted. Admin oversees all the data and grants access to a particular piece of data only to relevant Project Managers and Area Managers for each case.

	The recipient is only IECAH and the data is never transferred to third parties unless legally required by authorities, in which case prior authorisation will be requested from the contracting authority (EACEA), as defined in article II.9.2 of the Framework Contract. **ACI BLUETEAM** Organisational measures: - Adoption of the Personal Data Protection Regulation; - Nomination of the Personal Data Protection Officer (DPO); - Nomination of system administrators; - Training of employees on the processing of personal data and instruction regarding the use of electronic tools; - Nomination of personal data processing managers; - Information on the processing of data relating to travel management and organization. Technical measures: - Physical access control (access with keys or code, alarm, video surveillance) - IT access control (Active Directory, centralized identity provider) - Network protection systems (Firewall, VPN, etc.) - Client device protection (patch management, antivirus, antimalware, MDM, etc.) - Redundancy and backup of servers and databases - Data breach management policy - Regulation on the use of IT tools **THE DATA CONTROLLER (EACEA)** The European Commission's IT systems used by EACEA abide by the Commission's security guidelines. The Agency must comply with Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission. 1. Organisational measures: A Corporate Local Informatics Security Officer (C-LISO) is in place. Its role includes supervising the Agency compliance with the relevant regulations, and the application of security measures recommend by DIGIT. Organisational measures include appropriate access rights and access control. As a rule within the Agency, access to information systems, the file system or offices are subject to a series of authorisations where the person granting the access is different from the person requesting or authorising the access - except in limited cases of delegation. The responsible person in the unit in charge of this action (processing operation of the current record) collects and places the documents on the secured drives of the Commission and all Agency staff are bound by a confidentiality obligation. The need to know principle applies in all cases. 2. Technical measures: State of the art technical cybersecurity measures are implemented in the corporate systems, according to the security needs. Those measures are in constant evolution.
14	**Information to data subjects / Data Protection Notice (DPN)**
	The European Voluntary Humanitarian Aid Corps Training Data Protection Notice is available in the European Youth portal: https://youth.europa.eu/solidarity_en and data subjects will have access to it once they are logged in.